In the Claims:

Please amend the Claims as follows:

1. (Canceled)

2. (Currently Amended) The method as defined in Claim ~~1~~ 25 wherein the Plaintext checksum, the Ciphertext checksum and the universal hash value are all of the same size.

3. (Previously Presented) The method as defined in Claim 2 wherein the size of the first of the plurality of Plaintext blocks is a multiple of the size of the universal hash value.

4. (Previously Presented) The method as defined in Claim 3, further comprising computing a partial sum by taking the exclusive-or sum of the plurality of Plaintext blocks and reducing the partial sum to obtain the Plaintext checksum.

5. (Previously Presented) The method as defined in Claim 4 wherein reducing the partial sum comprises computation of the exclusive-or sum of equal sized segments of the partial sum.

6. (Previously Presented) The method as defined in Claim 3, further comprising:

reducing the plurality of Plaintext blocks to obtain a plurality of partial Plaintext blocks; and

combining the plurality of partial Plaintext blocks using an exclusive-or sum to obtain the Plaintext checksum.

7. (Previously Presented) The method as defined in Claim 6 wherein reducing the plurality of Plaintext blocks comprises the computation of the exclusive-or sum of equal sized segments of the Plaintext blocks.

8. (Previously Presented) The method as defined in Claim 3 wherein obtaining the Ciphertext checksum comprises:

selecting partial Ciphertexts using the third key from each of the plurality of Ciphertext blocks; and

combining the partial Ciphertexts using an exclusive-or sum to obtain the Ciphertext checksum.

9. (Previously Presented) The method as defined in Claim 8 wherein selecting partial Ciphertexts using the third key from a Ciphertext block comprises the process of using the bits of the third key as an index into the Ciphertext block.

10. (Currently Amended) ~~The method as defined in Claim 9, further comprising:~~ A method for generating a simple universal hash value, the method comprising:

inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a corresponding plurality of Ciphertext blocks;

computing a Plaintext checksum value responsive to each of the plurality of Plaintext blocks;

processing the plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum responsive to each of the corresponding plurality of Ciphertext blocks;

combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value;

dividing the Ciphertext block into a plurality of equal sized segments;

assigning each one of a plurality of bits from the third key to each of the plurality of segments, respectively;

selecting a single bit from the assigned segment in correspondence with the plurality of bits of the third key; and

concatenating the plurality of single bits selected from each of the segments to obtain the partial Ciphertext.

wherein the Plaintext checksum, the Ciphertext checksum and the universal hash value are all of the same size,

wherein the size of the first of the plurality of Plaintext blocks is a multiple of the size of the universal hash value,

wherein obtaining the Ciphertext checksum comprises:

selecting partial Ciphertexts using the third key from each of the plurality of Ciphertext blocks,

combining the partial Ciphertexts using an exclusive-or sum to obtain the Ciphertext checksum, and

wherein selecting partial Ciphertexts using the third key from a Ciphertext block comprises the process of using the bits of the third key as an index into the Ciphertext block.

11. (Previously Presented) The method as defined in Claim 3 wherein the Plaintext checksum and the Ciphertext checksum are combined by an exclusive-or operation to obtain the universal hash value.

12. (Previously Presented) The method as defined in Claim 3 wherein obtaining the Ciphertext

checksum comprises:

obtaining partial checksums using known universal hash functions from the third key and each of the plurality of Ciphertext blocks; and

combining the partial checksums using an exclusive-or sum to obtain the Ciphertext checksum.

13. (Canceled)

14. (Currently Amended) The apparatus as defined in Claim ~~13~~ 26 wherein the Plaintext checksum, the Ciphertext checksum and the universal hash value are each of the same size.

15. (Previously Presented) The apparatus as defined in Claim 14 wherein the size of the first of the plurality of Plaintext blocks is a multiple of the size of the universal hash value.

16. (Previously Presented) The apparatus as defined in Claim 15, further comprising Plaintext checksum means for computing a partial sum by taking the exclusive-or sum of the plurality of Plaintext blocks and reducing the partial sum to obtain the Plaintext checksum.

17. (Previously Presented) The apparatus as defined in Claim 16 wherein the Plaintext checksum means reduces the partial sum by computation of the exclusive-or sum of equal sized segments of the partial sum.

18. (Previously Presented) The apparatus as defined in Claim 15 wherein the plurality of Plaintext blocks is reduced to obtain a plurality of partial Plaintext blocks, which, in turn, are combined using an exclusive-or sum to obtain the Plaintext checksum.

19. (Previously Presented) The apparatus as defined in Claim 18 wherein the plurality of Plaintext blocks is reduced by computation of the exclusive-or sum of equal sized segments of the Plaintext blocks.

20. (Previously Presented) The apparatus as defined in Claim 15, further comprising means for obtaining the Ciphertext checksum by selecting partial Ciphertexts using the third key from each of the plurality of Ciphertext blocks, and combining the partial Ciphertexts using an exclusive-or sum to obtain the Ciphertext checksum.

21. (Previously Presented) The apparatus as defined in Claim 20 wherein the selection of a partial Ciphertext using the third key from a Ciphertext block includes using the bits of the third key as an index into the Ciphertext block.

22. (Currently Amended) ~~The apparatus as defined in Claim 21~~ A simple universal hashing apparatus comprising:

input means for inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a corresponding plurality of Ciphertext blocks;

Plaintext checksum means for computing a Plaintext checksum value responsive to each of said plurality of Plaintext blocks;

Ciphertext checksum means for processing said plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum responsive to each of said corresponding plurality of Ciphertext blocks;

combination means for combining the said Plaintext checksum and the said Ciphertext checksum to obtain the simple universal hash value; and

means for obtaining the Ciphertext checksum by selecting partial Ciphertexts using the third key from each of the plurality of Ciphertext blocks, and combining the partial Ciphertexts using an exclusive-or sum to obtain the Ciphertext checksum.

wherein:

the Plaintext checksum, the Ciphertext checksum and the universal hash value are each of the same size;

the size of the first of the plurality of Plaintext blocks is a multiple of the size of the universal hash value;

the selection of a partial Ciphertext using the third key from a Ciphertext block includes using the bits of the third key as an index into the Ciphertext block;

the Ciphertext block is divided into a plurality of equal sized segments;

each one of a plurality of bits of the third key is assigned to each of the plurality of segments, respectively;

the plurality of bits of the third key are used to select a single bit from the assigned segment; and

the plurality of single bits selected from each of the segments is concatenated to obtain the partial Ciphertext.

23. (Previously Presented) The apparatus as defined in Claim 15, further comprising an exclusive-or unit for combining the Plaintext checksum and the Ciphertext checksum to obtain the universal hash value.

24. (Currently Amended) A program storage memory readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for generating a simple universal hash value, the program steps comprising:

inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a corresponding plurality of Ciphertext blocks;

computing a Plaintext checksum value responsive to each of said plurality of Plaintext blocks;

~~processing said plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum responsive to each of said corresponding plurality of Ciphertext blocks; and~~

dividing at least one of the plurality of Ciphertext blocks into a plurality of equal sized segments;

assigning each one of a plurality of bits from a third key to each of the plurality of segments, respectively;

selecting a single bit from an assigned segment in correspondence with the plurality of bits of the third key; and

concatenating a plurality of single bits selected from each of the segments to obtain a partial Ciphertext;

combining partial Ciphertexts using an exclusive-or sum to obtain a Ciphertext checksum; and

combining ~~the~~ said Plaintext checksum and ~~the~~ said Ciphertext checksum to obtain the simple universal hash value.

25. (Currently Amended) A method for generating a simple universal hash value, the method comprising:

inputting at least one of a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a plurality of Ciphertext blocks;

computing a Plaintext checksum value from the plurality of Plaintext blocks;

~~processing the plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum;~~

~~combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value;~~

dividing at least one of the plurality of Ciphertext blocks into a plurality of equal sized segments;

assigning each one of a plurality of bits from a third key to each of the plurality of segments, respectively;

selecting a single bit from an assigned segment in correspondence with the plurality of bits of the third key; ~~and~~

concatenating a plurality of single bits selected from each of the segments to obtain a partial Ciphertext;

combining partial Ciphertexts to obtain a Ciphertext checksum; and

combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value.

26. (Currently Amended) A simple universal hashing apparatus comprising:

input means for inputting at least one of a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a plurality of Ciphertext blocks;

Plaintext checksum means for computing a Plaintext checksum value from ~~the~~ said plurality of Plaintext blocks;

Ciphertext checksum means for processing said plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum; and

combination means for combining ~~the~~ said Plaintext checksum and ~~the~~ said Ciphertext checksum to obtain the simple universal hash value,

wherein:

at least one of said plurality of Ciphertext blocks is divided into a plurality of equal sized segments;

each one of a plurality of bits of a third key is assigned to each of the plurality of segments, respectively;

the plurality of bits of the third key are used to select a single bit from the assigned segment; ~~and~~

a plurality of single bits selected from each of the segments is concatenated to obtain ~~the~~ a partial Ciphertext; and

partial Ciphertexts are combined to obtain the Ciphertext checksum.

27. (New) A method as defined in Claim 25 wherein the partial Ciphertexts are combined using an exclusive-or sum.

28. (New) An apparatus as defined in Claim 26 wherein the partial Ciphertexts are combined using an exclusive-or sum.